



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/784,391

02/15/2001

Kevin C. Jones

EWG-076

3000

23735 7590 05/05/2004

DIGIMARC CORPORATION  
19801 SW 72ND AVENUE  
SUITE 250  
TUALATIN, OR 97062

EXAMINER

AKHAVANNIK, HUSSEIN

ART UNIT

PAPER NUMBER

2621

DATE MAILED: 05/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/784,391

Applicant(s)

JONES, KEVIN C.

Examiner

Hussein Akhavannik

Art Unit

2621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☒ Claim(s) 2 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>11</u> . | 6) <input type="checkbox"/> Other: ____.  |

## **DETAILED ACTION**

### ***Response to Amendment***

1. The amendments to the specification overcome the Examiner's objections cited in paragraph 1 of the previous office action (now Paper No. 9).
2. The amendments to claims 2 and 7-11 overcome the Examiner's objections cited in paragraph 2 of the previous office action (now Paper No. 9).
3. The amendments to claims 4 and 10 overcome the Examiner's 35 USC 112, second paragraph rejection of claims 4 and 10-12 cited in paragraph 6 of the previous office action (now Paper No. 9).

### ***Drawings***

4. The drawings were received on February 12, 2004. These drawings are accepted.

### ***Response to Arguments***

5. Applicant's arguments, see page 10, lines 6-12 of the Remarks, filed 2/12/2004, with respect to claims 1-2 have been fully considered and are persuasive. The 35 USC 102(e) rejection of claims 1-2 has been withdrawn.

The Applicant alleges that Thorne et al in view of Rhoads fail to teach a program for reading watermarks in documents that form at least part of the messages and documents attached to the messages. The Examiner respectfully disagrees. Rhoads explains that the bodier replaces the need for a header by placing the information "traditionally stored in the header into the digital signal and empirical data itself" in column 41, lines 20-26. In the system of Thorne et al and Rhoads, the empirical data corresponds to the document that makes up the e-mail message, as explained by Thorne et al in column 7, lines 21-33 and column 9, lines 54-67. Thorne et al

Art Unit: 2621

add a header to the document in order to control the distribution of the message (corresponding to the e-mail, which is made up of the header and the document). Thus, by replacing the header explained by Thorne et al by the body of Rhoads, the information contained in the header will be embedded in the document (corresponding to the empirical data) that forms at least part of the messages of Thorne et al steganographically.

The Applicant alleges that Thorne et al in view of Rhoads fail to disclose or suggest a watermark detecting means for detecting and reading watermarks in e-mail messages at the server after the messages are sent from the user but before the messages are transmitted from the e-mail server to the Internet. The Examiner agrees that Thorne et al in view of Rhoads fail to disclose such a feature. However, Gibbs illustrates an authenticated message server 112 in figure 1 that reads information contained in e-mails to control distribution of the e-mails before the e-mails are transmitted to the Internet (explained in column 6, lines 28-37). By rejecting the messages if they are not authenticated before they are sent to the Internet, the authenticated message server reduces the probability that an unauthorized user will ever access the message (because the message never enters public or third-party domains). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to detect and read watermarks in e-mail messages, as suggested by Thorne et al in view of Rhoads, at the server after the messages are sent from the user but before the messages are transmitted from the e-mail server to the Internet, as suggested by Gibbs, because the probability of the e-mails reaching an unauthorized user would be reduced.

The Applicant alleges that Kasiraj et al fail to teach or suggest the interrogation of a database to determine an action to take with a particular message based at least in part on the

Art Unit: 2621

data carried by the watermark. The Examiner respectfully disagrees. Though Kasiraj et al do not explicitly disclose a database being interrogated, they do explain that electronic message profiles are stored (“previously established”) to “automatically control the delivery and receipt of its associated electronic message” in the abstract. In order to store an electronic message profile (data) for each electronic message, it is inherent that the data must be stored in a database.

The Applicant alleges that Kasiraj et al analyze the restrictions upon receipt of an electronic message, whereas claim 7 describes an approach for controlling distribution prior to transmission. The Examiner agrees that Kasiraj et al do illustrate that the electronic message profiles are analyzed after they are received by a user. However, Thorne et al explain that the software for reading the header of an e-mail (corresponding to a watermark) and restricting the transmission of an e-mail may be located on the e-mail server in column 8, lines 43-58. Thorne et al explain that this system is beneficial so that the potential capability of defeating the security procedures is reduced due to unpredictable problems. In this embodiment the database integration program of Kasiraj et al (as explained in the abstract and illustrated in figure 5) would also be located on the e-mail server in order to apply the proper restrictions to e-mail delivery. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the database interrogation program of Kasiraj et al upon receipt into the e-mail server of Thorne et al and Rhoads so that the potential capability of defeating the security procedures is reduced due to unpredictable problems.

#### ***Claim Objections***

6. Claim 2 is objected to because of the following informalities:

Art Unit: 2621

In claim 2, lines 1-2, "A system which includes an e-mail server connected to the Internet" should have either "consisting of" or "comprising" appended, in order to correctly separate the heading of the claims with the body.

Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 5-9 and 15-16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Referring to claims 5 and 15-16, reading watermarks in "documents in and attached to the messages" is not understood. On page 4, line 20 to page 5, line 11 of the specification, the Applicants explain that a document in a message may be watermarked or ("In still another alternative embodiment instead of having an image 11 embedded in the message") a document being attached to the message may be watermarked in two separate embodiments. There is no single embodiment which explains that both a document in the message and attached to the message may be watermarked. Thus, the Applicant is advised to change "in and attached" to "in or attached".

Art Unit: 2621

Referring to claim 6-9, these claims are rejected for depending from an indefinite antecedent base claim.

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thorne et al (U.S. Patent No. 5,958,005) in view of Rhoads (U.S. Patent No. 5,862,260).

Referring to claim 1,

- i. An electronic messaging system including a mail server which sends and receives messages is illustrated by Thorne et al in figure 1 by the e-mail servers 112 and 114.
- ii. The mail server including a watermark reading program which reads watermarks in the messages is not explicitly explained by Thorne et al. Thorne et al do explain inspecting the header of an e-mail in order to determine whether the e-mail is secure in column 9, lines 54-59 and illustrate the inspecting in figure 5A by reference number 518. Rhoads explains that a "bodier" can be used to replace a header in column 41, lines 20-40. By using such a bodier, the header cannot be simply stripped off in an attempt to remove the confidential flag in a header (as illustrated by Thorne et al in figure 4), as the bodier is embedded within the empirical data steganographically. Thus, by replacing the header of Thorne et al by the bodier as explained by Rhoads, the security of the imperceptibility and robustness of the header information would be increased. Therefore,

it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a mail server include a watermark reading program which reads watermarks in messages in order to determine the flags of a header which has been stored as a watermark (bodier).

iii. The program operable to read watermarks in documents that form at least part of the messages and documents attached to the messages is not explicitly explained by Thorne et al. However, Rhoads explains that the bodier replaces the need for a header by placing the information “traditionally stored in the header into the digital signal and empirical data itself”, corresponding to claim 1ii. In the system of Thorne et al and Rhoads, the empirical data corresponds to the document that makes up the e-mail message, as explained by Thorne et al in column 7, lines 21-33 and column 9, lines 54-67. Thorne et al add a header to the document in order to control the distribution of the message (corresponding to the e-mail, which is made up of the header and the document). Thus, by replacing the header explained by Thorne et al by the bodier of Rhoads, the information contained in the header will be embedded in the document (corresponding to the empirical data) that forms at least part of the messages of Thorne et al steganographically.

iv. The program operable to control the distribution of the messages in response to the data in the watermarks is explained by Thorne et al in column 7, lines 34-42. The system of Thorne et al will erase or delete an e-mail when the “confidential” flag is raised in the header (which corresponds to a watermark as explained in claim 1ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also



control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

Referring to claim 3,

- i. A system for controlling the distribution of electronic messages that contain confidential information is illustrated by Thorne et al in figure 3.
- ii. Each electronic message that having confidential information including a digital watermark carrying data that indicates that the message is confidential is not explicitly explained by Thorne et al. Thorne et al do illustrate a header that contains a confidentiality field in figure 4. However, Rhoads explains that a “bodier” can be used to replace a header corresponding to claim 1ii.
- iii. A server which transmits and receives messages is illustrated by Thorne et al in figure 1 by the e-mail servers (112 and 114).
- iv. The server including a watermark reading program which reads watermarks in messages and controls the distribution of such messages in accordance with the data carried by any watermarks in the messages is explained by Thorne et al in column 7, lines 34-42. The server of Thorne et al will erase or delete an e-mail when the “confidential” flag is raised in the header (which corresponds to a watermark as explained in claim 3ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

- v. The program operable to read watermarks in documents that form at least part of the messages and documents attached to the messages corresponds to claim 1iii.

Referring to claim 4, the messages being transmitted over the Internet is explained by Thorne et al in column 5, lines 54-67.

Referring to claim 5,

- i. Controlling the distribution of electronic messages that include confidential information is illustrated by Thorne et al in figure 3.
- ii. The messages including digital watermarks that carry data indicating that the message contains confidential information is not explicitly explained by Thorne et al. Thorne et al do illustrate a header that contains a confidentiality field in figure 4. Rhoads explains that a “bodier” can be used to replace a header, corresponding to claim 1ii.
- iii. Reading the watermarks in messages prior to transmission of the messages is explained by Thorne et al in column 8, lines 43-58. Thorne et al explain that the e-mail software is installed only on the e-mail server, so that the header (corresponding to the watermark) is read, as illustrated in figure 5A by step 518, at the server before the messages are transmitted to a user.
- iv. Reading watermarks in documents in and attached to the message corresponds to claim 1iii.
- iv. Controlling the distribution of each electronic message which contains a watermark in response to the data carried by the watermark in the message is explained by Thorne et al in column 7, lines 34-42. The server of Thorne et al will erase or delete an e-mail when the “confidential” flag is raised in the header (which corresponds to a

Art Unit: 2621

watermark as explained in claim 5ii), thereby ending the distribution of the e-mail.

Furthermore, additional flags in the header also control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

Referring to claim 6, the messages being transmitted over the Internet corresponds to claim 4.

11. Claims 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thorne et al in view of Rhoads, and further in view of Gibbs (U.S. Patent No. 6,615,348).

Referring to claim 2,

i. A means for transmitting messages from an individual user to an e-mail server is illustrated by Thorne et al in figure 1 by the user workstations (118 and 120) connected to the e-mail server (112).

ii. A watermark detecting means for detecting and reading watermarks in e-mail messages at the server after the messages are sent from the user but before the messages are transmitted from the e-mail server to the Internet is not explicitly explained by Thorne et al. Thorne et al do explain inspecting the header of an e-mail in order to determine whether the e-mail is secure in column 9, lines 54-59 and illustrate inspecting the header in figure 5A by reference number 518. Rhoads explains that a "bodier" can be used to replace a header, corresponding to claim 1ii. Gibbs illustrates an authenticated message server 112 in figure 1 that reads information contained in e-mails to control distribution of the e-mails before the e-mails are transmitted to the Internet (explained in column 6, lines 28-37). By rejecting the messages if they are not authenticated before they are sent

Art Unit: 2621

to the Internet, the authenticated message server reduces the probability that an unauthorized user will ever access the message (because the message never enters public or third-party domains). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to detect and read watermarks in e-mail messages, as suggested by Thorne et al in view of Rhoads, at the server after the messages are sent from the user but before the messages are transmitted from the e-mail server to the Internet, as suggested by Gibbs, because the probability of the e-mails reaching an unauthorized user would be reduced.

iii. A means for preventing the transmission of messages from the e-mail server to the Internet of the watermark detecting means detects a watermark which has an indication that the message containing the watermark is confidential is explained by Thorne et al in column 7, lines 34-42. The system of Thorne et al will erase or delete an e-mail when the "confidential" flag is raised in the header (which corresponds to a watermark as explained in claim 2ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12. By deleting the message at the authenticated message server, corresponding to claim 2ii, the messages will not be transmitted to the Internet in the system of Thorne et al, Rhoads, and Gibbs.

12. Claims 7-13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thorne et al in view of Rhoads, and further in view of Kasiraj et al (EP Patent Application Pub. No. 0,375,138).

Referring to claim 7, a database being interrogated to determine an action to take with a particular message based at least in part on the data carried by a watermark is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. Such interrogation is performed to control distribution of electronic messages to recipients which meet certain criteria. By interrogating the database of Kasiraj et al when the confidential flag (located in the data carried by the watermark) of Thorne et al and Rhoads is raised, the security of the e-mail server of Thorne et al and Rhoads would be improved. Thorne et al explain that the software for reading the header of an e-mail (corresponding to a watermark) and restricting the transmission of an e-mail may be located on the e-mail server in column 8, lines 43-58. Thorne et al explain that this system is beneficial so that the potential capability of defeating the security procedures is reduced due to unpredictable problems. In this embodiment the database integration program of Kasiraj et al (as explained in the abstract and illustrated in figure 5) would also be located on the e-mail server in order to apply the proper restrictions to e-mail delivery. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made interrogate a database to determine the action to take (send or not send) with a particular message based at least in part on the data carried by the watermark and to implement the database interrogation program of Kasiraj et al upon receipt into the e-mail server of Thorne et al and Rhoads, so that the potential capability of defeating the security procedures is reduced due to unpredictable problems and the security of e-mail distribution in the network of Thorne et al and Rhoads is improved.

Art Unit: 2621

Referring to claim 8, the action taken with respect to a particular message being dependent of the identity of the sender, the identity of the receiver, and information carried by the watermark is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. The profile is explained to include the recipient's security classification, the identifying information of the source (sender) and the content of the e-mail (which will include the bodier of the system of Thorne et al and Rhoads). By using the identity of the sender, the identity of the receiver, and information carried by the watermark, a database can be interrogated to control distribution of electronic messages to recipients that meet certain criteria. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the identity of the sender, the identity of the receiver, and information carried by the watermark when interrogating a database to determine the action to take (send or not send) with a particular message in order to improve the security of e-mail distribution in the network of Thorne et al and Rhoads.

Referring to claim 9, the action taken with respect to a particular message being dependent on the identity of the sender, the identity of the receiver, information carried by the watermark, and information stored in a database is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. The profile is further explained to include the recipient's security classification, the identifying information of the source (sender) and the content of the e-mail (which will include the bodier of the system of Thorne et al and Rhoads). By using the identity of the sender, the identity of the receiver, and

Art Unit: 2621

information carried by the watermark, a database can be interrogated to control distribution of electronic messages to recipients that meet certain criteria. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the identity of the sender, the identity of the receiver, and information carried by the watermark when interrogating a database to determine the action to take (send or not send) with a particular message in order to improve the security of e-mail distribution in the network of Thorne et al and Rhoads.

Referring to claim 10,

- i. Detecting and reading digital watermarks carried in such messages to determine how flags in such watermarks are set is not explicitly explained by Thorne et al. Thorne et al do explain inspecting the header of an e-mail in order to determine whether the e-mail is secure in column 9, lines 54-59 and illustrate the inspecting in figure 5A by reference number 518. Thorne et al also explain that the field of the header correspond to flags in column 8, lines 28-42. Rhoads explains that a "bodier" can be used to replace a header, corresponding to claim 1ii.
- ii. Interrogating a database to determine what action should be taken with a message based upon the identity of the sender, the identity of the receiver and the flag setting in the watermark in the message corresponds to claim 8.

Referring to claim 11, the messages being transmitted over the Internet corresponds to claim 4.

Art Unit: 2621

Referring to claim 12, the data carried by the watermark indicating if the message contains confidential information is illustrated by Thorne et al in figure 4 by the confidential field of the header, which is used to create the bodier (corresponding to claim 10i).

Referring claim 13,

- i. Detecting and reading digital watermarks carried in such message to determine information carried in the watermarks cooresponds to claim 10i, wherein the flag settings are the information carried in the watermarks.
- ii. Interrogating a database to determine what action should be taken with a message based at least in part upon the information in the watermark corresponds to claim 10ii.

Referring to claim 15, detecting and reading being performed on documents in or attached to the messages corresponds to claim 1iii.

13. Claims 14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thorne et al in view of Rhoads and Kasiraj et al, and further in view of Gibbs.

Referring to claim 14, the detecting and reading of the digital watermarks being performed in a server separate from a source and destination of the messages is not explicitly explained by Thorne et al or Rhoads or Kasiraj et al. However, Gibbs illustrates an authenticated message server 112 in figure 1 that reads information contained in e-mails to control distribution of the e-mails before the e-mails are transmitted to the Internet (explained in column 6, lines 28-37). By rejecting the messages if they are not authenticated before they are sent to the Internet, the authenticated message server reduces the probability that an unauthorized user will ever access the message (because the message never enters public or third-party domains). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made



Art Unit: 2621

to detect and read watermarks in e-mail messages, as suggested by Thorne et al in view of Rhoads and Kasiraj et al, at the server after the messages are sent from the user but before the messages are transmitted from the e-mail server to the Internet, as suggested by Gibbs, because the probability of the e-mails reaching an unauthorized user would be reduced.

Referring to claim 16, detecting and reading being performed on documents in or attached to the messages corresponds to claim 1iii.

### *Conclusion*

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hussein Akhavannik whose telephone number is (703)306-4049. The examiner can normally be reached on M-F 8:30-5:00.

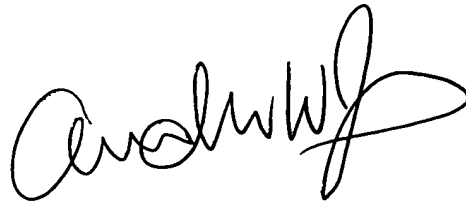
Art Unit: 2621

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Leo H. Boudreau can be reached on (703)305-4706. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Hussein Akhavannik  
May 3, 2004

HA.



**ANDREW W. JOHNS**  
**PRIMARY EXAMINER**